Predator Connect W6x
Dual-band Wi-Fi 6 Router

User Manual _v1.0

Revision May, 2024

Contents

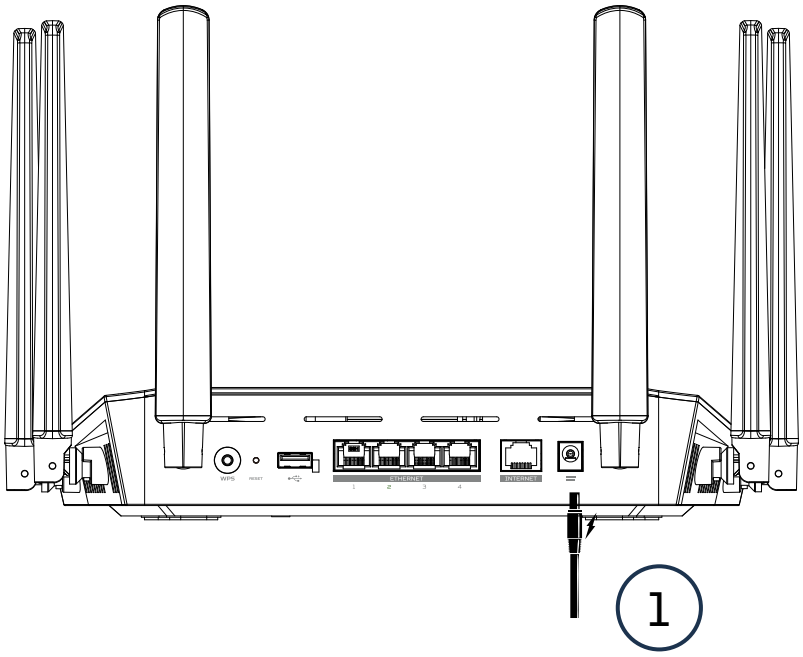
1. Overview. 3
2. Installation and Setup. 3
3. Initial Configuration 6
3.1 Dashboard 7
4. Hybrid QoS 9
5. WiFi 11
5.1 Basic Settings 11
5.2 Guest WiFi 12
5.3 Smart Home WiFi 12
5.4 WPS 13
5.5 ACS (Automatic Channel Selection) 13
5.6 Advanced Settings 13
5.7 WiFi MAC Filter 14
6. LAN 14
7. Home Network Security. 15
7.1 Network Security Setting 15
7.2 Parental Control 16
8. WAN 17
8.1 WAN status 17
8.2 WAN setting 17
8.3 DMZ 18
8.4 Port forwarding 18
8.5 VPN server 19
8.6 Firewall 20
8.7 WAN ping 20
8.8 DDNS 20
9. IPv6 21
10. System 21
10.1 Firmware update 21
10.2 Login password 21
10.3 Backup and restore 22
10.4 System log 22
10.5 System time 23
10.6 Main LED 23
10.7 System Information 24
10.8 Restart and Reset default 24
10.9 Languages 24
10.10 USB storage. 25
11. Troubleshooting 26
11.1 Quick Tips 26
11.2 FAQs (Frequently Asked Questions) 26
12. Appendix factory default settings 27
13. Router Basic Specification 28
14. Regulatory Information 29

1. Overview

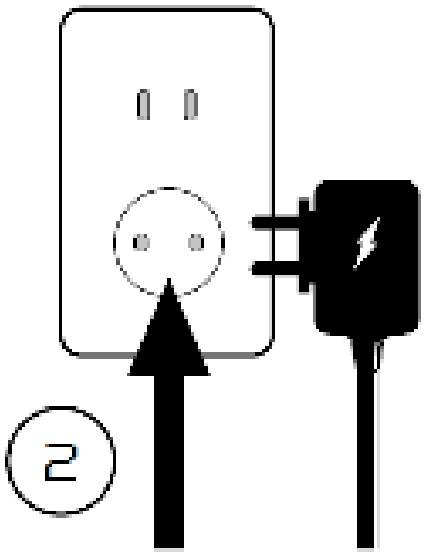
Predator Connect series W6, a whole new Wi-Fi 6 Dual-band wireless router, is optimized for gamers with intensive features and simple setup steps via a 1-2-3 wizard. A new stylish 6-antenna desktop wireless router tuned for optimal gaming experience and for your household. Network Security protection is embedded. Live updates ensure your network is immune from malware and vulnerability threats 24-7. Smart home (IoT) devices can be setup on their own WiFi network. ACS (Automatic Channel Selection) dynamically chooses the most suitable channel for the W6x when you experience interference from nearby 5GHz SSIDs. Port forwarding profiles for most game consoles (PS5, XBOX, etc.) are readily available inside for gameplay. Hybrid QoS is the best fit for your Predator router, ensuring prioritization of your gaming traffic and bandwidth utilization. The VPN feature provides a secure connection for your device when surfing the website.

2. Installation and Setup

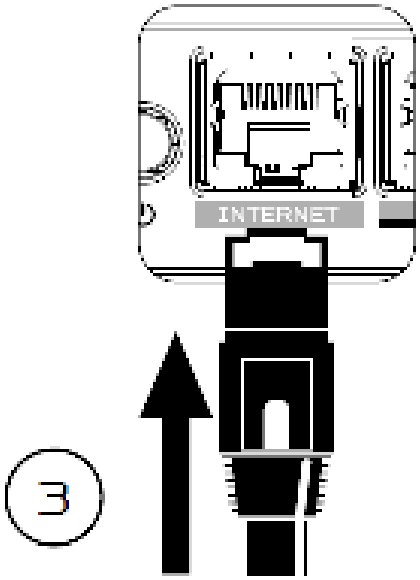
2.1. Plug in AC adapter.



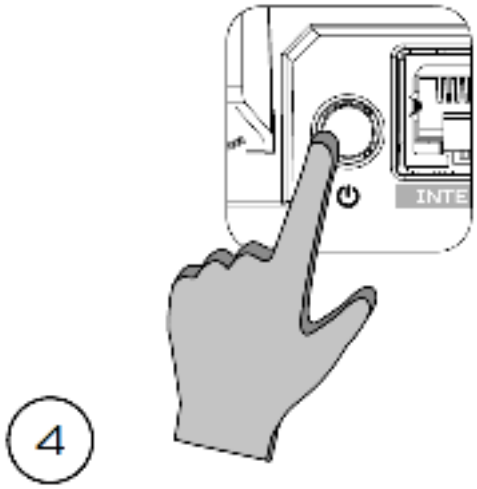
2.2. Plug into outlet.



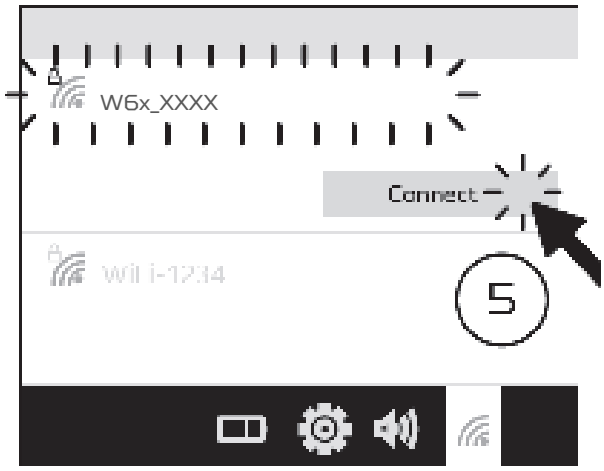
2.3 Plug in Internet cable.



2.4 Power on device.



2.5 Connect to PredatorW6x WiFi.



2.6 Important information is at the bottom of the device.

Setup the router via browser:

- Please make sure that the wireless function on your laptop is already enabled.
- Check the device bottom label, and find the router default SSID (W6x_XXXX) and password and then connect.
- Open the browser on your laptop/desktop, input the device web admin URL: http://acer-connect.com or IP: http://192.168.76.1
- The device will automatically redirect to a quick setup wizard. Follow the easy 1-2-3 steps and get ready to access the internet.

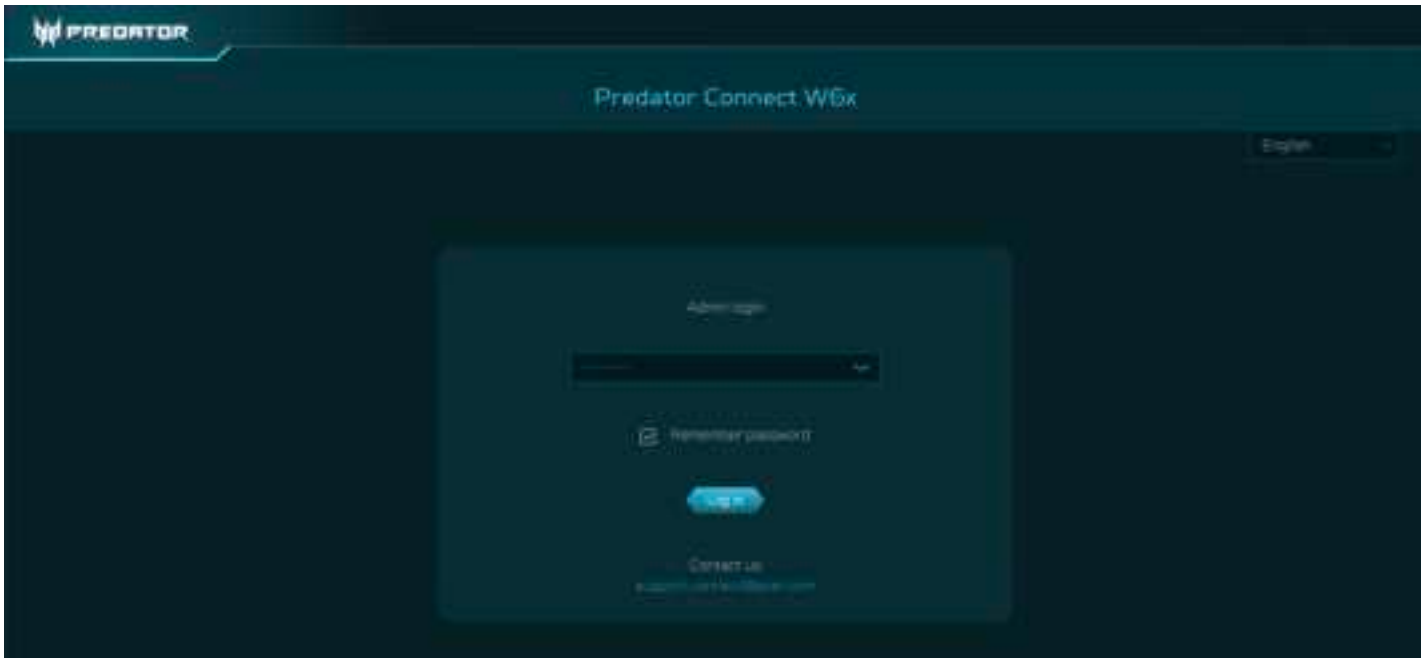
Note: The admin login password requires modification within the setup wizard for a first Time use. Please create a strong password and keep it in a safe place. (New password cannot be same as the prior one.)

Note: The router web admin portal will automatically lock after five consecutive incorrect attempts. You have to power cycle the router to unlock the web admin.

Note: The SSID WiFi password can't be same as admin login password.

3. Initial Configuration

Please log in to the Predator Connect W6x Web Portal (http://acer-connect.com or IP: http://192.168.76.1) by using the current valid Admin password. You can select the language of Web UI by clicking on the dropdown arrow.



Enter the login password to see the dashboard and other settings of your Predator Connect W6x. The router will automatically guide you step by step how to setup and configure internet access and basic network settings.

3.1 Dashboard

Once you have successfully logged in, the following key information will be displayed on the Predator Connect W6x dashboard.

Connection Status: shows the current connection status of Internet.

WAN Status: shows WAN connectivity and Download/Upload speed and WAN IP.

WiFi Status: shows number of wireless client devices connected with 2.4GHz and 5GHz bands.

LAN Status: quickly indicates the status of LAN ports. Predator Connect W6x has one WAN port, one Game port and three LAN ports i.e. LAN 1, LAN 2, LAN 3.

The "icon" (at the left) represents the number of devices connected to the W6x router. Clicking on this icon will display the table shown below.

System Up time: shows system up time since last reboot.

Connected Devices: shows how many client devices are connected with your Predator Connect W6x through WiFi or LAN.

You can also modify the device name by clicking on the pencil icon.

This tab displays client device name, IP address allocated by the router, MAC address of the device, mode of connection (whether the device is connected with router through Ethernet or WiFi), and duration of device connectivity with the router. You can even block the device from accessing the Internet by clicking on "block" button.

Network Traffic: helps indicate real time status of the Download (DL) and Upload (UL) speeds across the WAN.

Network Speed Test:

1) Powered by SPEEDTEST.

A single push of the “Start” button tests the speed of the WAN connectivity.

2) You can even manually select the server option. Click on the dropdown arrow and it will display the available servers.

3) Clicking the “start” Button will test the network speed and display the results as shown in the image below.

It will test and clearly show the network download and upload speed in Mbps, ping rate and jitter in milliseconds.

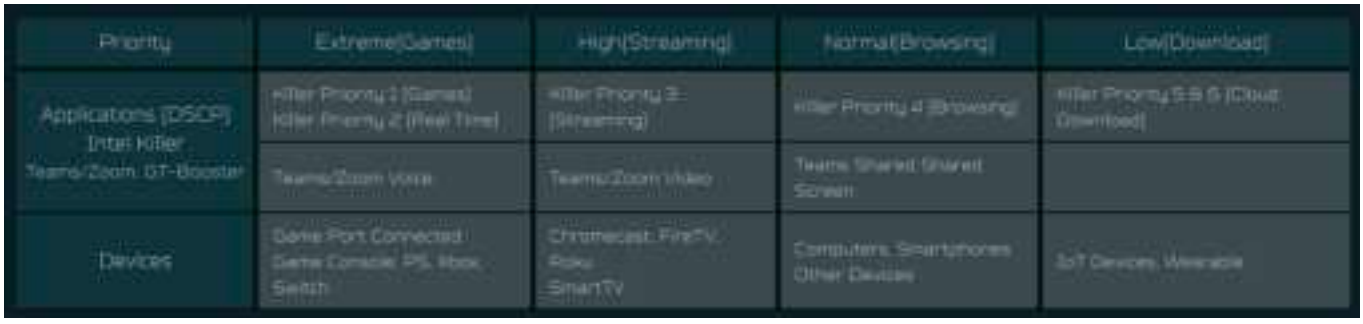
After getting the speed test results, you have the option to run the speed test again.

4. Hybrid QoS

Hybrid QoS combines application priority and device priority. The Killer-Enabled PC can set applications priority and send packets with DSCP values to the Predator Connect W6x router, then the router will classify packets and set priority for all different applications based on the below definition.

For non-Killer-Enabled devices, Predator Connect W6x can identify game consoles, streaming devices, computers, and smartphones and IoT devices in the network and allocate them to priority group according to the default settings, or the user can manually set priority for devices connected to the route.

*Note: Device identification requires network security engine option enable.
Application based QoS* priority.
*Note: Application Priority will use the DSCP value in the IP header for packet classification. Laptop/desktop with Killer™ embedded traffic priorities in four grades by application. I.e. Extreme (Games), High (Streaming), Normal (Browsing), Low (Download).



Device priority:
Note 1: Killer-Enabled PC is set to default extreme priority whether connected by wired Ethernet or by wireless.
Note 2: You may drag and drop connected clients into the desired priority level. The change is effective immediately.

For the upload and download **bandwidth** configuration, please contact your ISP to get the exact value of upload and download bandwidth. Once the bandwidth is configured, QoS will reserve the bandwidth according to the weighting percentage of each priority queue.

You may select “use default configuration” and click on “Apply”. Otherwise, you can select “setting manually” and enter the required upload and download bandwidth with priority weighting.

5. WiFi

WiFi Status
Displays key information such as:
• WiFi SSID
• SSID Broadcast
• Security
• Channel
• Connected devices
• Gateway address
• Mac address of 2.4GHz, 5GHz

5.1. Basic Settings

In this page, you can edit WiFi SSID and enable or disable SSID broadcast and use the following security parameters for 2.4GHz and 5GHz bands

WPA, WPA2, WPA/WPA2, WPA3 personal, WPA2/WPA3, Enhanced open;

Encryption option: AES, Auto, TKIP. Auto and TKIP are available only, when WPA, WPA/WPA2 security option applied.

Host Band Steering: a feature designed to optimize your Wi-Fi network by automatically directing your devices to the best available frequency band. This helps ensure that each device receives the strongest possible signal and the best performance.

5.2. Guest WiFi

This tab provides information about the Internet connection for guests and their devices accessing your network.

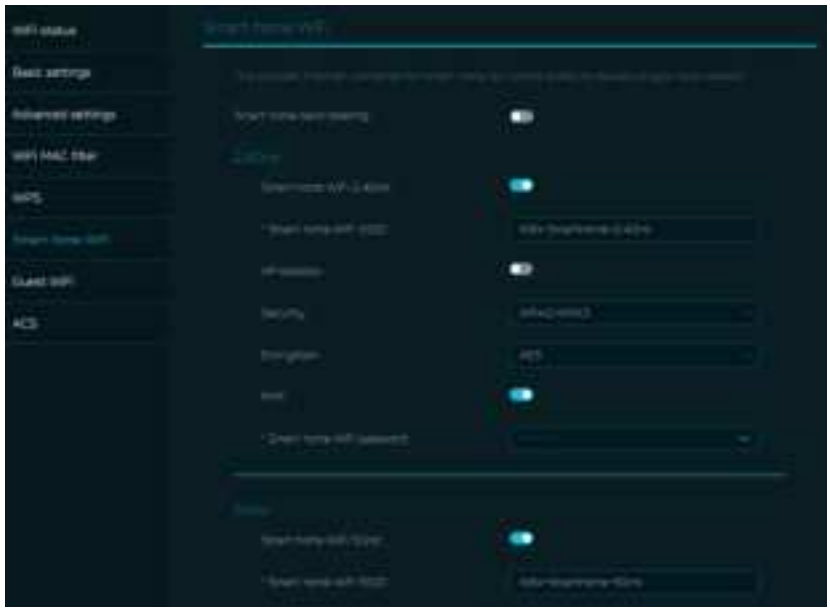
When enabling Guest WiFi on any band, it will ask to provide Guest WiFi SSID and security parameters. You can select security and encryption option by clicking drop down arrows.

Guest WiFi password is set by default for all bands, so it is suggested to change the passwords for security reasons.

5.3. Smart home WiFi

This tab provides Internet connection for smart home WiFi, but blocks access to devices on your local network.

Choose to enable between 2.4GHz/ 5GHz band and set the WiFi SSID and security parameters for smart home WiFi.



5.4. WPS

WPS (WiFi Protected Setup) provides an easy way to connect your device to the network by pushing the WPS button.

On this page, you can configure the WPS (Wi-Fi Protected Setup) settings for the 2.4 GHz and 5 GHz bands.
In this page, you can configure the WPS settings of 2.4GHz and 5GHz bands.
Steps to Configure WPS:
1, Initiate WPS Setup: Click on “Start WPS”.
2, Activate WPS on Your Device: Within two minutes, enable WPS on your wireless device.

5.5. ACS (Automatic Channel Selection)

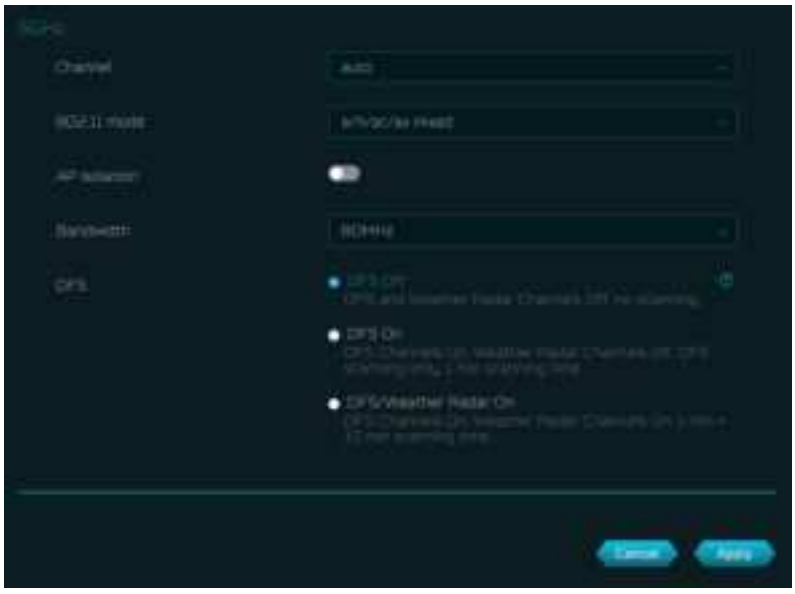
ACS is a mechanism to optimize the channel assignment. It selects the best working channel dynamically. One that is clear and has the least traffic.

Note 1: There will be a small delay, rescanning and then cycling OFF and ON if the client is associated within the ACS enablement band. Please check your device wireless connection and select the best WiFi W6x router SSID after ACS process is completed.
Note 2: The ACS is not applicable if all the bands (2.4GHz, 5GHz) are configured as fixed channel.

5.6 Advanced Settings
This tab will help you to setup advanced WiFi parameters for 2.4GHz and 5GHz bands.

AP isolation is a feature that enables you to create a separate virtual network preventing client communicating with each other and preventing unwanted hacking. This feature is disabled by default.

DFS (Dynamic Frequency Selection) is a function of using 5GHz Wi-Fi frequencies that are generally reserved for radar, such as satellite communication, weather radar etc.



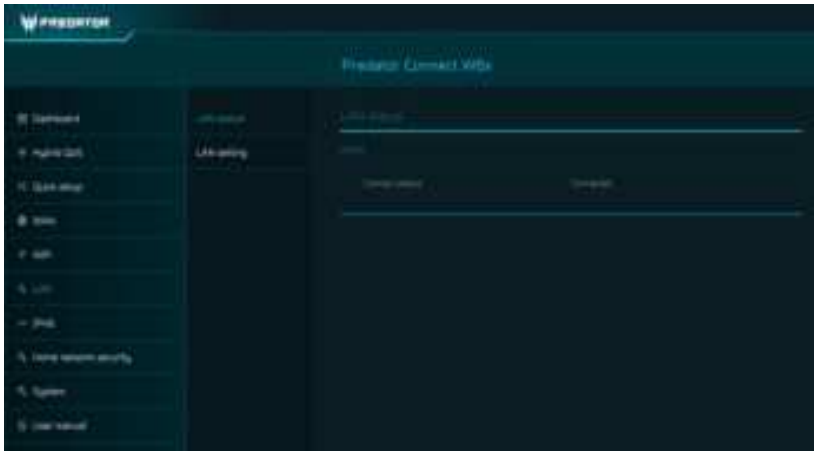
5.7 WiFi MAC filter
Devices which are added in WiFi MAC filter will be blocked from accessing the Internet.

Click on (+) icon to add the device in filter table by entering its name & MAC address. Up to 32 devices can be added in the MAC filter table.

6 . LAN

LAN status

In this page, the LAN Status section provides a comprehensive overview of both WAN and LAN connections. This section displays key information about the status and connectivity of your network.

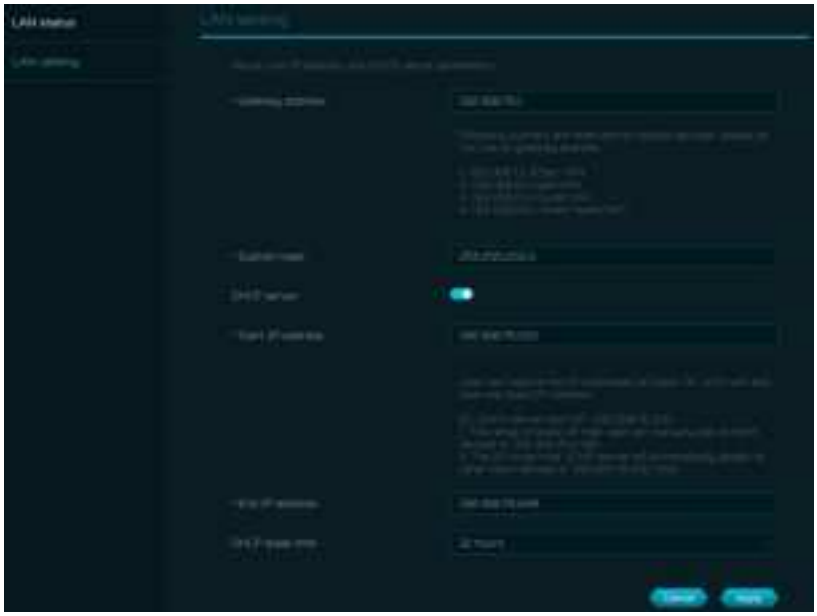


WAN Status: Shows the status of the Wide Area Network (WAN) connection. It includes details such as the IP address and MAC address assigned to the WAN interface.
If the WAN is connected, you will see the current IP address.

LAN Status: Provides information about the Local Area Network (LAN) connections. It displays the IP address and MAC address for each device connected to the LAN ports.
.

LAN Setting

This tab allows you to setup LAN IP gateway address with an option to enable or disable DHCP server feature.



You can enter/edit gateway address and subnet mask.
DHCP server provides and assigns IP addresses,
default gateways and other network parameters to client devices. DHCP server can be enabled or disabled as per the network requirement.

Following subnets are reserved for default services. Please do not use as gateway address.

1. 192.168.7.x(IPsec VPN)
2. 192.168.8.x (Open VPN)
3. 192.168.10.x (Guest WiFi)
4. 192.168.20.x (Smart Home WiFi)

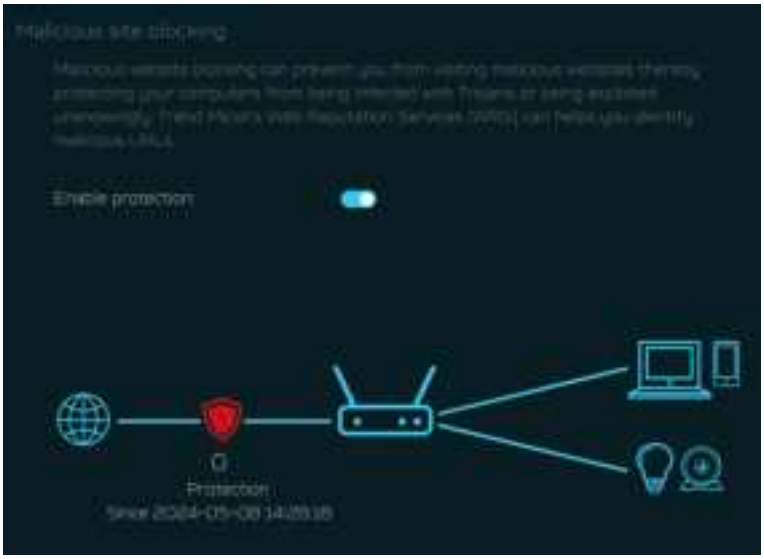
7 . Home Network Security

Home network security tab includes network security setting and web and app controller within parental control feature. These two features must accept the Trend Micro license agreement before enablement.

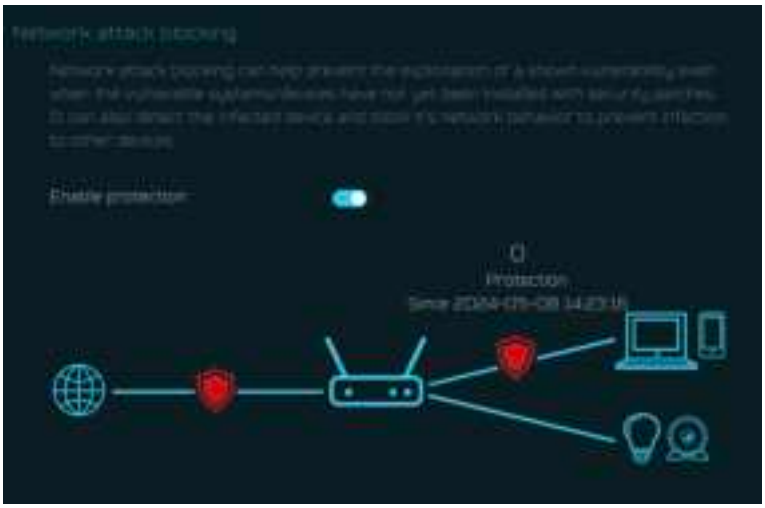
7.1 Network Security Setting

This tab contains network security related information, powered by Trend Micro, where you can turn on/off the security engine and enable protection against malicious sites, network attacks and harmful connections coming from IoT devices.

Malicious site blocking prevents from unwanted sites to open and hence protecting your computer from being infected with Trojans. There is a feature called “Trend Micro’s Web Reputation Service (WRS) that identifies malicious URLs and allow you to take action against infected URLs.



By enabling **Network attack blocking** feature, the router detects the infected devices and block its network behavior to prevent infection to other devices.



Enabling **IoT security**

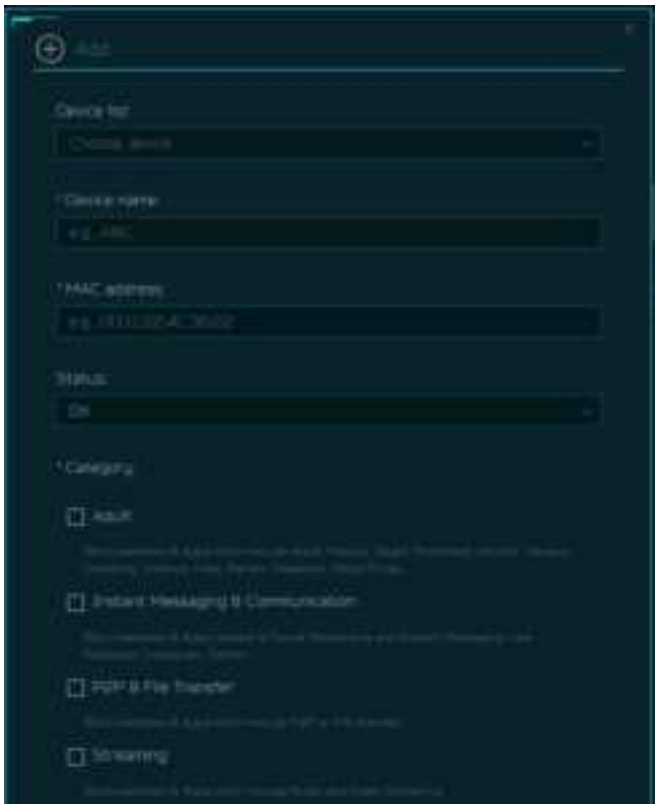
protection feature detects and blocks harmful connections from compromised IoT devices by using Trend Micro's smart protection network.

It's a continuously updated IoT device reputation database that prevents the network from false connections.

7.2 Parental Control

This feature allows you to control and block unwanted sites on specific devices.
You can enable/disable Web & App controller.

Once you click on (+) icon, following window will appear and here you can enter device list, device name, its MAC address, status and select the following categories for blocking websites.



- **Adult**

Block websites and Apps which include Adult, Mature, Illegal, Prohibited, Alcohol, Tobacco, Gambling, Violence, Hate, Racism, Weapons, Illegal Drugs related content.

- **Instant Messaging and Communication**

Block websites and Apps related to Social Networking and Instant Messaging like Facebook, Instagram, Twitter etc.

- **P2P and File Transfer**

Block websites and Apps which include P2P or File transfer.

- **Streaming**

Block websites and Apps which include Audio and Video streaming.

8. WAN

8.1 WAN Status
This tab provides information about WAN connectivity status and following key information:

- Time duration (format HH:MM:SS)
- MAC address
- Connection Mode: DHCP, static IP, PPPoE, switch WAN port to LAN (switch/bridge).
- IP address
- Subnet mask
- Default gateway
- Primary & Secondary DNS server

8.2 WAN Setting:
In this page, you can set up Ethernet WAN connection mode to DHCP, Static IP, PPPoE or switch WAN port to LAN, depending on your connection usage.

Click on down arrow to reveal the drop-down menu to select your preferred WAN settings. You can select “Switch WAN port to LAN (Switch/Bridge mode)”, if you are using the router in repeater mode in which the WAN port is not required. As a result, you can have one more LAN port.

Note: After switching to Bridge mode,
1) Please disable the DHCP Server on the Predator Connect W6x according to your network topology.
2) Some functions may not work as how it does in router mode. E.g. Home network security, Hybrid QoS, Guest WiFi, Smart Home WiFi, IPv6, DMZ, Firewall, Port forwarding, VPN, WAN ping, WAN setting.
3) To access Predator Connect W6x’s web portal, it is recommended to setup IP under your client network device and connect to W6x via Ethernet cable. The LAN gateway of W6x should also be configured as the client network device’s gateway and DNS server.

8.3 DMZ

DMZ is a physical or logical sub network that contains and exposes firm's facing services to an untrusted, usually larger, network such as the Internet.

If external users can't access certain network services provided by the Local Area Network (LAN), use the DMZ function to set the client that provides the required network services as the DMZ host. DMZ host IP address needs to be entered and then external users will have access to all services.

8.4 Port Forwarding

This feature allows external users to connect to Local Area Network (LAN) services using Hypertext Transfer Protocol (HTTP), File transfer protocols (FTP), and other protocols.
To add any application, click on (+) icon and select a required service.

You can select any service profile from common services tab and it will then automatically show its name, LAN & WAN port number and its protocol.

Enter the LAN IP address and select the status ON/OFF and click on "Apply" button to activate the service.

New game console profiles have been Added, including:

- Xbox network
- Play Station 5
- Play Station 4
- Nintendo SWITCH
- Nvidia GeForce Now
- Steam

8.5 VPN Server

Setup VPN server on Predator Connect W6x for remote VPN connection over the Internet. This router offers two VPN services:

-OpenVPN
-IPsec VPN

User needs to generate certificate before enabling VPN server. Once you create a VPN server, VPN connection link establish and status with be shown. It will display the connection type, remote & local IP address and duration.

Open VPN is a SSL VPN and uses a chosen UDP or TCP port, allowing for flexible configuration choices.
User access comes with two different options; Home network, Internet and home network.

User can also export OpenVPN configuration file (client.ovpn).

IPsec VPN uses predefined communication channels, UDP 500 and UDP 4500, to establish the encrypted tunnel and ESP for the transmission of encrypted data.

8.6 Firewall

Setup firewall rule to accept or drop network request from Internet.
In order to setup a firewall, click on (+) icon and enter the name, source and destination port and IP address, protocol, target and status info.

8.7 WAN Ping

By enabling this feature, WAN port of Predator Connect W6x will respond to ping requests that are sent to the WAN IP address from the Internet.

For better security, keep this feature turned OFF, and the device will not respond to a WAN ping.

8.8 DDNS

A DDNS service provides a fixed domain name for your router's dynamic IP address. You will need to register with a DDNS services among the following ones.

1. No IP
2. Google domain
3. Cloudflare.com

9. IPv6

You can setup IPv6 settings from this tab.

The Predator Connect W6x supports IPv6 mode below: DHCPv6, static IPv6, PPPoE, 464xlat, 6rd, DS-Lite. Connection mode will be disabled by default.

Please consult local Internet Service Provider before enabling and configuring the option.

10. SYSTEM

10.1 Firmware Update
In this tab, you can check the existing firmware version and also click on “check new”, to see if there is an update available.

10.2 Login Password
You can change the login password of your Predator Connect W6x from this page.

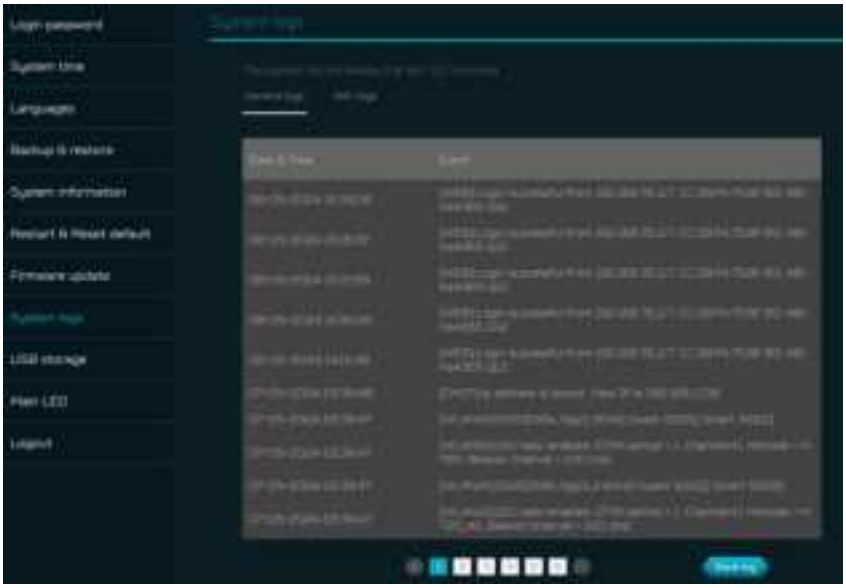
To make a new password, you need to enter current password first. Please use a strong password to keep it secure.

10.3 Backup and Restore
In this tab, you can check how to save the configuration:
Click on "Backup" to backup current device configuration. On both Windows and MAC OS, this is saved to your 'Downloads' folder.

How to restore the configuration:
1) Click Browse to select a file
2) Click Restore

10.4 System Log

General log will display here all the latest 100 activities you have done with the router.



WiFi logs will display the WiFi status and its setting data.

You can save the system log by clicking the “Save log” button at the bottom of the page.

10.5 System Time

This tab allows you to synchronize the device time with the system time by enabling “Automatically set time zone”.

By enabling “daylight savings time”, device will automatically adjust the time according to the time zone.

10.6 Main LED

This tab displays information about LED colors and its indication. These LED indicators will help you to know and understand router behavior.

Congestion Detection test helps you to identify the Internet connection status; whether it is good, normal or poor. Different LED lights will indicate different statuses.

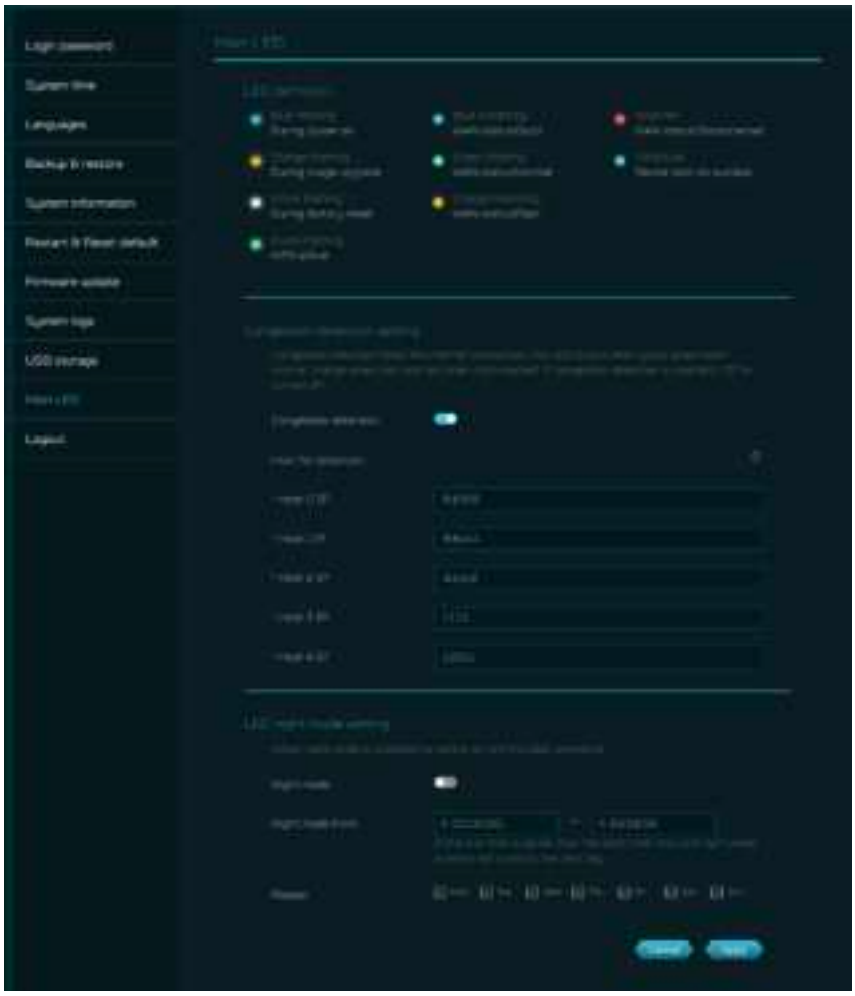
LED is OFF, if congestion detection is disabled.

Enter the host IP addresses for detection.

Enabling **LED night mode**, only dims the device luminance.

Please check if you have already setup the correct time zone (auto/manual), before enabling this option.

You can setup the daily schedule as needed.



10.7 System Information

It shows key device information of Predator Connect W6x, such as:

- Device name
- Serial number
- Firmware version
- Web version

10.8 Restart and Reset Default
From this tab, you can click on "Restart device" to reboot the router and click on "Factory data reset" to restore factory default settings.

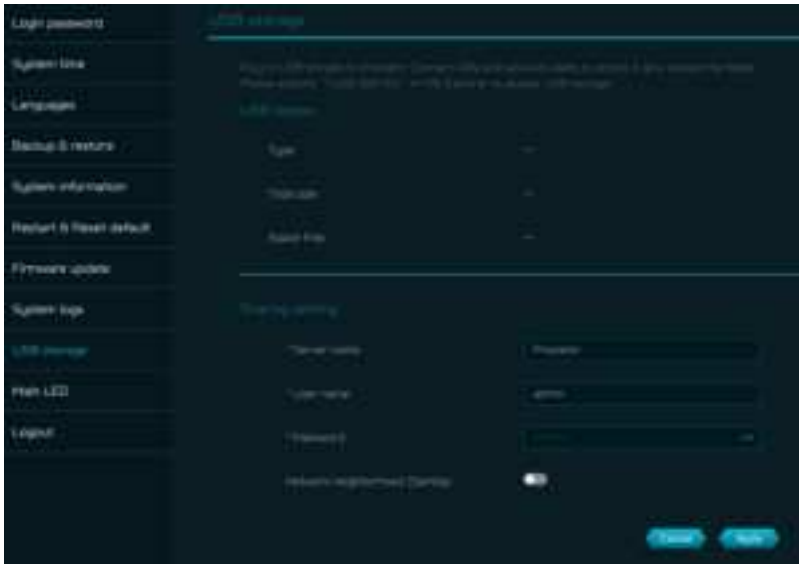
10.9 Languages
You can select the language of your Predator Connect W6x from this tab.

10.10 USB Storage
This router has a USB port where you can plug in a USB drive and allow all authorized users to access the files on your USB drive.

Once you plug in USB drive, it will display device type, size and free space available.

Enter the Server name and login credentials for shared access to USB drive.

In sharing setting, there is an option to enable/disable Network neighborhood (Samba).



11. Troubleshooting

11.1 Quick tips

This section describes common issue which you can encounter.

Sequence to restart the device and network:

1. Turn off and unplug the router power plug.
2. Turn off the W6x router.
3. Plug in the router power plug and then turn it on. Wait for two minutes till the router LED steady as before.
4. Turn on the W6x router and wait for the device upper deck main LED steady breathing.

11. 2 Frequently Asked Questions (FAQs)

11.2.1 What can I do if I forget my wireless password?

- Connect to the W6x router via Ethernet cable LAN.
- Visit device portal http://acer-connect.com and login admin.
- Go to WiFi -> Basic settings/Retrieve or reset the WiFi passwords.

11.2.2 What can I do if I forget the router's web portal admin password?

Reset the device by pressing and holding the reset key until the LED start blinking white. After the device restore to factory default, please login web admin portal with admin PWD, label printed on bottom of the device.

Note 1: The device web admin will be locked after 5 wrong password attempts. The user is required to reboot the device to disable the web admin.
Note 2: Remember to setup the device internet connection after reset. Remember to also change the admin password.

11.2.3 What can I do if I can't log into router's web admin portal?

Please follow the steps below to check on your client's device.

- Check whether the client allocated IP and DNS server IPs both are with same subnet and gateway.
- Clean the browser cookies or use private/Incognito mode to access the router admin.

11.2.4 What can I do if I can't surf the internet even though the configuration is finished?

Please follow the step below to check on your W6x router:

- Login to the web admin portal dashboard to check Internet status.
- Continuingly, if the Internet status is up and connect. Go to WAN setting, manually configure DNS server using below IP and apply:

  Primary DNS server: 8.8.8.8
  Secondary DNS server: 8.8.4.4
- If the issue still there, please restart the modem and router accordingly.

12. Appendix Factory Default Setting

Router web admin	
URL	http://acer-connect.com http://acerconnect.com http://192.168.76.1
Login password (case-sensitive)	XXXXXXX (XXXX is randomized variables. Please check device bottom label)
Local Network (LAN)	
Gateway address	192.168.76.1
Subnet mask	255.255.255.0
DHCP server	192.168.76.1
DHCP range	192.168.76.100 to 192.168.76.254
Time zone	Depends on country or region you bought the router.
DHCP starting IP address	192.168.76.100
DHCP ending IP address	192.168.76.254
Time adjusted for daylight save time	Enabled.
Wireless LAN (WLAN)	
WiFi SSID (case-sensitive)	2.4 GHz : W6x-YYYY-2.4GHz 5 GHz : W6x-YYYY-5GHz (YYYY is randomized variables. Please check device bottom label)
Security	2.4 GHz : WPA2/WPA3 5 GHz : WPA2/WPA3
SSID Broadcast	Enabled.
Country / Region	United States in the US; otherwise, varies by region.
RF channel	2.4 GHz : Auto 5 GHz : Auto
Default operation mode (with AX enabled)	2.4 GHz : Up to 600 Mbps 5 GHz : Up to 4804 Mbps
Guest WiFi	Disabled.
Smart Home WiFi	Disabled.
Home Network Security	Disabled.

13. Router Basic Specification

Processor	Quad A53 2.0GHz	
Memory	RAM	1GB
	Storage	256MB
Wireless LAN	IEEE standard	802.11 a/b/g/n/ac/ax
	MU-MIMO	4x4 MIMO
	Band	Dual band, 2.4/5GHz
	Throughput	AX6000
Ethernet	WAN	1 x 2.5Gbps
	LAN	4 x 1Gbps
USB	Port	USB 3.0 Type-A
	Storage	FTP, Samba
Button Key	WPS	Yes, WPS and Mesh pairing
	Reset	Yes, Factory reset
LED	LED	LED *1
Form factor	Dimension	270mm x 187mm x 49.5mm
	Weight	1016g
DC Power Jack	Input Voltage	AC 100-240V, 50-60Hz, 1.6A
	Power Adapter	12V/2.5A, 30W

14. Regulatory Information

14.1 Important Safety Precaution

Your Predator Connect W6x Wi-Fi 6 Router device is manufactured to comply with European safety standards. This section outlines the safety precautions associated with using the device. Please read the safety and operation instructions before using your device and other accessories. Keep these instructions safe for future reference.

14.2 Condition of Use

- The device is not water-resistant. Please protect the device from water or moisture and do not touch the device with wet hands. Otherwise short-circuit and malfunction of the product or electric shock may occur.
- Keep the device and accessories in a cool, well- ventilated area and away from direct sunlight. Do not place the device in a container with poor heat dissipation. Do not enclose or cover your device with clothes, towels, or other objects.
- Put your device in places beyond the reach of children. Do not allow children to use the wireless device without guidance.
- Do not use your device at places for medical treatment (in an operating room, intensive care unit, or coronary care unit, etc.) where wireless device use is prohibited.
- To reduce the risk of accidents, do not use your device while driving.
- RF signals may affect the electronic systems of motor vehicles. For more information, consult the vehicle manufacturer.
- EE recommends using the charger supplied with your device. Use of another type of charger may result in malfunction and/or danger.

14.3 Cleaning and Maintenance

- Do not attempt to dry your device with an external heat source, such as a microwave oven or hair dryer.
- Use a clean, soft, and dry cloth to clean the device and accessories.

14.4 Disposal Instructions

Do not throw this electronic device into the trash when discarding. To minimize pollution and ensure utmost protection of the global environment, please recycle. For more information on the Waste from Electrical and

Electronics Equipment (WEEE) regulations, visit

www.acer-group.com/public/Sustainability

14.5 Ethernet Cable Line Safety

- Disconnect all Ethernet cable lines from the equipment when not in use and/or before servicing.
- To avoid the remote risk of electric shock from lightning, do not connect the Ethernet cable line to this equipment during lightning or thunderstorms.

14.6 Medical Devices

Operation of any radio transmitting equipment, including wireless phones, may interfere with the functionality of inadequately protected medical devices. Consult a physician or the manufacturer of the medical device to determine if they are adequately shielded from external RF energy or if you have any questions. Switch off your device in health care facilities when any regulations posted in these areas instruct you to do so. Hospitals or health care facilities may be using equipment that could be sensitive to external RF transmissions.

Pacemakers. Pacemaker manufacturers recommend that a minimum separation of 15.3 centimeters (6 inches) be maintained between wireless devices and a pacemaker to avoid potential interference with the pacemaker. These recommendations are consistent with the independent research by and recommendations of Wireless Technology Research. Persons with pacemakers should do the following:

- Always keep the device more than 15.3 centimeters (6 inches) from the pacemaker
- Not carry the device near you pacemaker when the device is switched on. If you suspect interference, switch off your device, and move it.

Hearing aids. Some digital wireless devices may interfere with some hearing aids. If interference occurs, consult your service provider.

14.7 Vehicles

RF signals may affect improperly installed or inadequately shielded electronic systems in motor vehicles such as electronic fuel injection systems, electronic antiskid (anti-lock) braking systems, electronic speed control systems, and air bag systems. For more information, check with the manufacturer, or its representative, of your vehicle or any equipment that has been added. Only qualified personnel should service the device, or install the device in a vehicle. Faulty installation or service may be dangerous and may invalidate any warranty that may apply to the device. Check regularly that all wireless

equipment in your vehicle is mounted and operating properly. Do not store or carry flammable liquids, gases, or explosive materials in the same compartment as the device, its parts, or enhancements. For vehicles equipped with an air bag, remember that air bags inflate with great force. Do not place objects, including installed or portable wireless equipment in the area over the air bag or in the air bag deployment area. If in-vehicle wireless equipment is improperly installed, and the air bag inflates, serious injury could result. Using your device while flying in aircraft is prohibited. Switch off your device before boarding an aircraft. The use of wireless devices in an aircraft may be dangerous to the operation of the aircraft, disrupt the wireless telephone network, and may be illegal.

14.8 Warning

- Do not attempt to open the device by yourself. Disassembling may result in damage to the device. Small parts may also present a choking hazard.
- When this device is switched on, it should be kept at least 15 cm from any medical device such as a pacemaker, a hearing aid or insulin pump, etc.
- Switch this device off when you are near gas or flammable liquids. Strictly obey all signs and instructions posted in any potentially explosive atmosphere.

14.9 Explosive Device Proximity Warning

Switch off your device when in any area with a potentially explosive atmosphere and obey all signs and instructions. Potentially explosive atmospheres include areas where you would normally be advised to turn off your vehicle engine. Sparks in such areas could cause an explosion or fire resulting in bodily injury or even death. Switch off the device at refueling points such as near gas pumps at service stations. Observe restrictions on the use of radio equipment in fuel depots, storage, and distribution areas; chemical plants; or where blasting operations are in progress. Areas with a potentially explosive atmosphere are often, but not always, clearly marked. They include below deck on boats, chemical transfer or storage facilities, vehicles using liquefied petroleum gas (such as propane or butane), and areas where the air contains chemicals or particles such as grain, dust or metal powders. Do not switch the notebook on when wireless phone use is prohibited or when it may cause interference or danger.

- Warning: Do not operate a portable transmitter (including this wireless adapter device) near unshielded blasting caps or in an explosive environment unless the transmitter has been modified to be qualifies for such use.

- Warning: The wireless adapter is not designed for use with high-gain directional antennas

14.10 Wireless adapter regulatory information

- Warning: For safety reasons, turn off all wireless or radio transmitting devices when using your device under the following conditions.

Remember to follow any special regulations in force in any area, and always switch off your device when its use is prohibited or when it may cause interference or danger. Use the device only in its normal operating positions. This device meets RF exposure guidelines when used normally. To successfully transmit data files or messages, this device requires a good quality connection to the network. In some cases, transmission of data files or messages may be delayed until such a connection is available. Parts of the device are magnetic. Metallic materials may be attracted to the device, and persons with hearing aids should not hold the device to the ear with the hearing aid. Do not place credit cards or other magnetic storage media near the device, because information stored on them may be erased.

Aircraft

Warning FCC and FAA regulations may prohibit airborne operation of radio-frequency wireless devices (wireless adapters) because their signals could interfere with critical aircraft instruments. Ask the airport staff and cabin crew before turning on your device's wireless adapter whilst on board.

The wireless adapter and your health

The wireless adapter, like other radio devices, emits radio frequency electromagnetic energy. The level of energy emitted by the wireless adapter, however, is less than the electromagnetic energy emitted by other wireless devices such as mobile phones. The wireless adapter operates within the guidelines found in radio frequency safety standards and recommendations. These standards and recommendations reflect the consensus of the scientific community and result from deliberations of panels and committees of scientists who continually review and interpret the extensive research literature. In some situations or environments, the use of the wireless adapter may be restricted by the proprietor of the building or responsible

representatives of the applicable organization. Examples of such situations may include:

• Using the wireless adapter on board airplanes, or

• Using the wireless adapter in any other environment where the risk of interference with other devices or services is perceived or identified as being harmful.

If you are uncertain of the policy that applies to the use of wireless adapters in a specific organization or environment (an airport, for example), you are encouraged to ask for authorization to use the adapter before you turn it on.

14.11 Statement

[USA]

- FCC regulations restrict the operation of this device to indoor use only.
- The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet.
- Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.
- This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.
This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

- This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and a human body.

[Canada — Industry Canada (IC)]
This device complies with RSS247 of Industry Canada.

- This device contains licence-exempt transmitter(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:
(1) this device may not cause interference,
(2) this device must accept any interference, including interference that may cause undesired operation of the device.

- L'émetteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :
(1) L'appareil ne doit pas produire de brouillage;
(2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

- This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and a human body.

- Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et un corps humain.

[NCC]
取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
應避免影響附近雷達系統之操作。
高增益指向性天線只得應用於固定式點對點系統。

14.12 EU Regulatory Conformance

List of applicable countries

This product must be used in strict accordance with the regulations and constraints in the country of use. For further information, contact the local office in the country of use. Please see **https://europa.eu/european- union/about-eu/countries_en** for the latest country list.

Specific absorption rate information

This device meets the EU requirements on the limitation of exposure of the general public to electromagnetic fields by way of health protection. The limits are part of extensive recommendations for the protection of the general public. These recommendations have been developed and checked by independent scientific organizations through regular and thorough evaluations of scientific studies. The unit of measurement for the European Council's recommended limit for mobile devices is the "Specific Absorption Rate" (SAR), and the SAR limit is 2.0 W/kg averaged over 10 grams of body tissue. It meets the requirements of the International Commission on Non-Ionizing Radiation Protection (ICNIRP). For body worn operation, this device has been tested and meets the ICNIRP exposure guidelines and the European Standard, for use with dedicated accessories. Use of other accessories which contain metals may not ensure compliance with ICNIRP exposure guidelines.

Hereby, Acer Incorporated declares that the radio equipment type W6x is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available: Please search for Predator Connect W6x Wi-Fi 6 Router at **www.acer.com**

14.13 Restrictions

Restriction or Requirement in the CE: 5150 to 5350 MHz indoor-use only.

	AT	BE	BG	CH	CY	CZ	DE
	DK	EE	EL	ES	FI	FR	HR
	HU	IE	IS	IT	LI	LT	LU
	LV	MT	NL	PL	PT	RO	SE
	SI	SK	TR	NO	UK(NI)		

WLAN 5GHz Band: For indoor use only.

	UK

14.14 EU Regulatory Compliance -- Radio

e.i.r.p power limit											
2.4G		5G(U-NII-1)		5G(U-NII-2a)		5G(U-NII-2b)		5G(U-NII-3)			
2400 MHz ~	2483.5 MHz	5150 MHz ~	5250 MHz	5250 MHz ~	5350 MHz	5470 MHz ~	5725 MHz	5725 MHz ~	5850 MHz		
e.i.r.p 20dBm		e.i.r.p 23dBm		e.i.r.p 20dBm		e.i.r.p 27dBm		e.i.r.p 13.98dBm			